

Figure 1
(Prior Art)

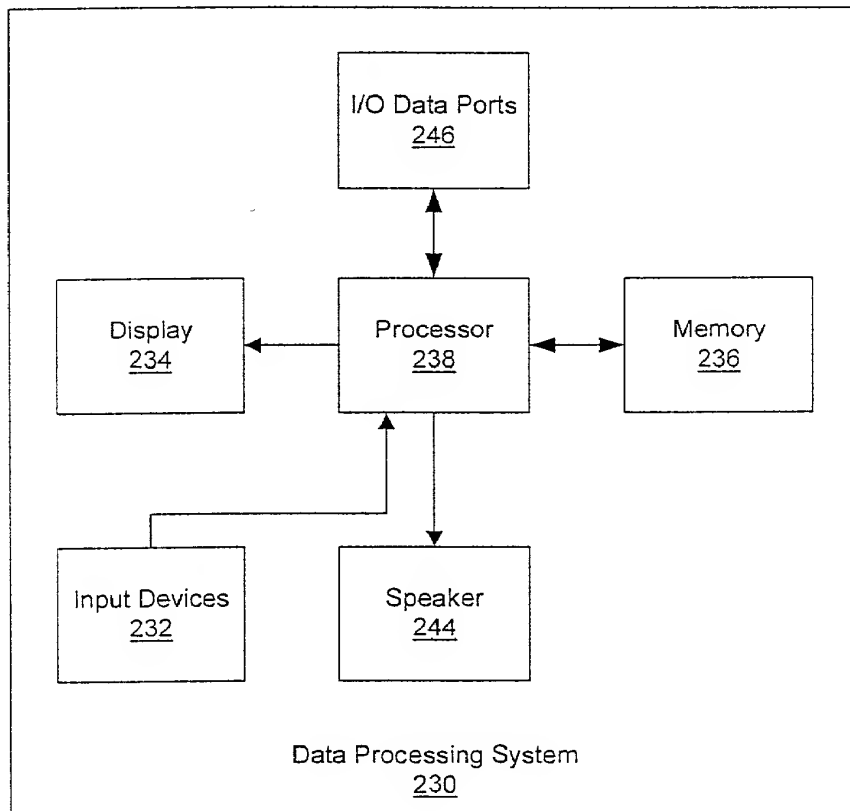


Figure 2

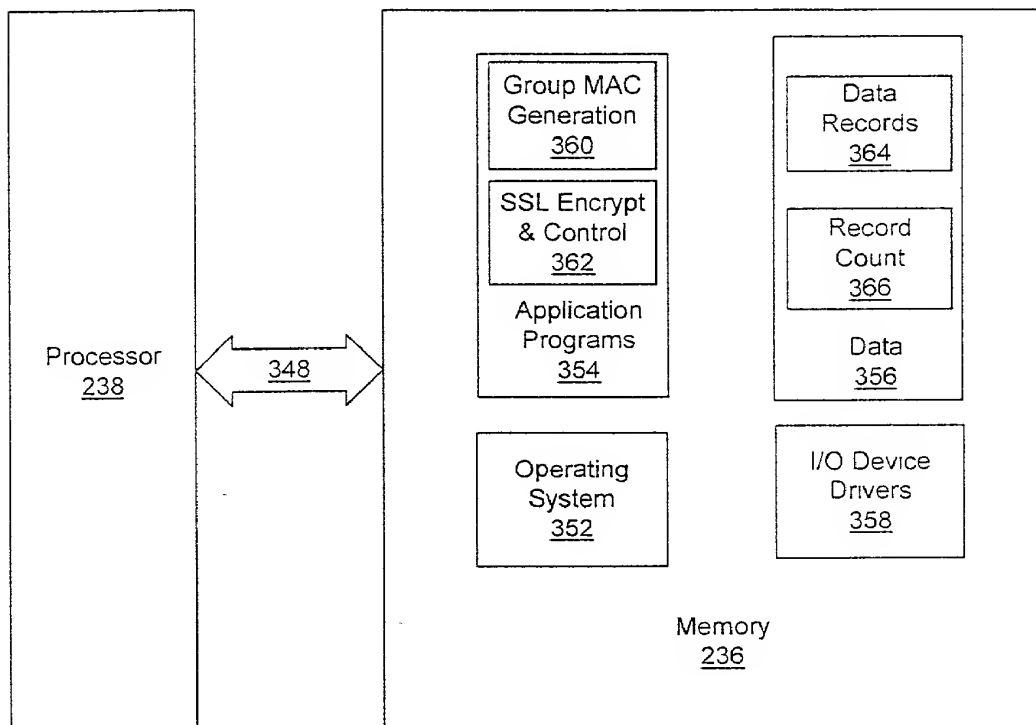


Figure 3

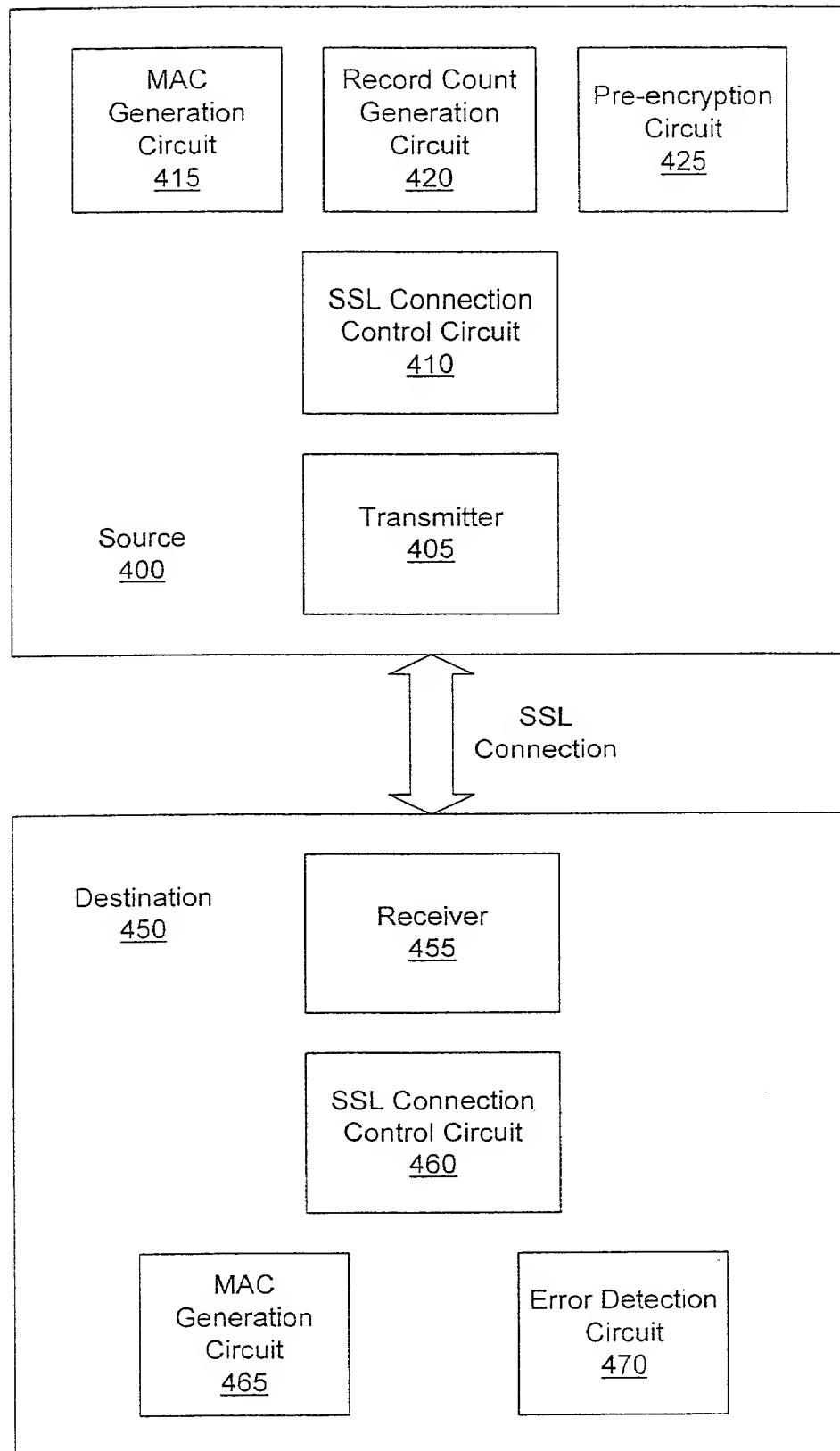


Figure 4

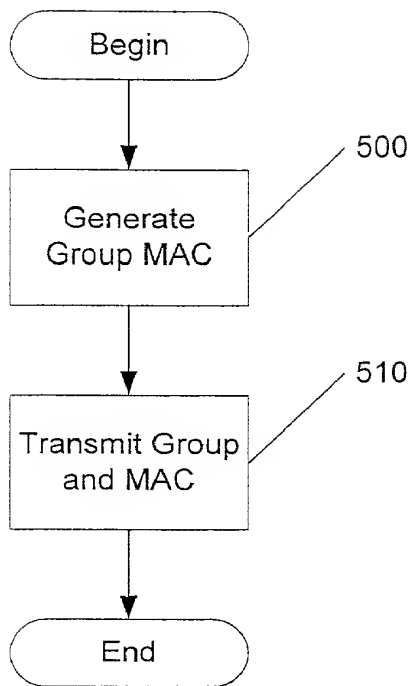


Figure 5

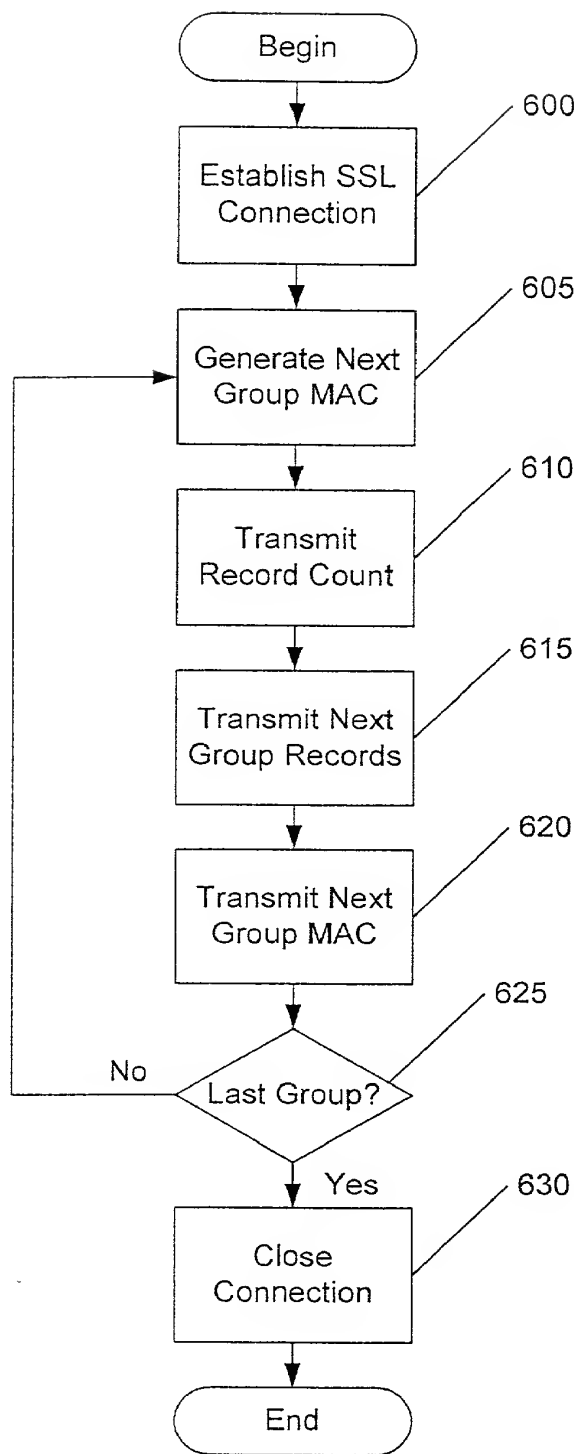


Figure 6

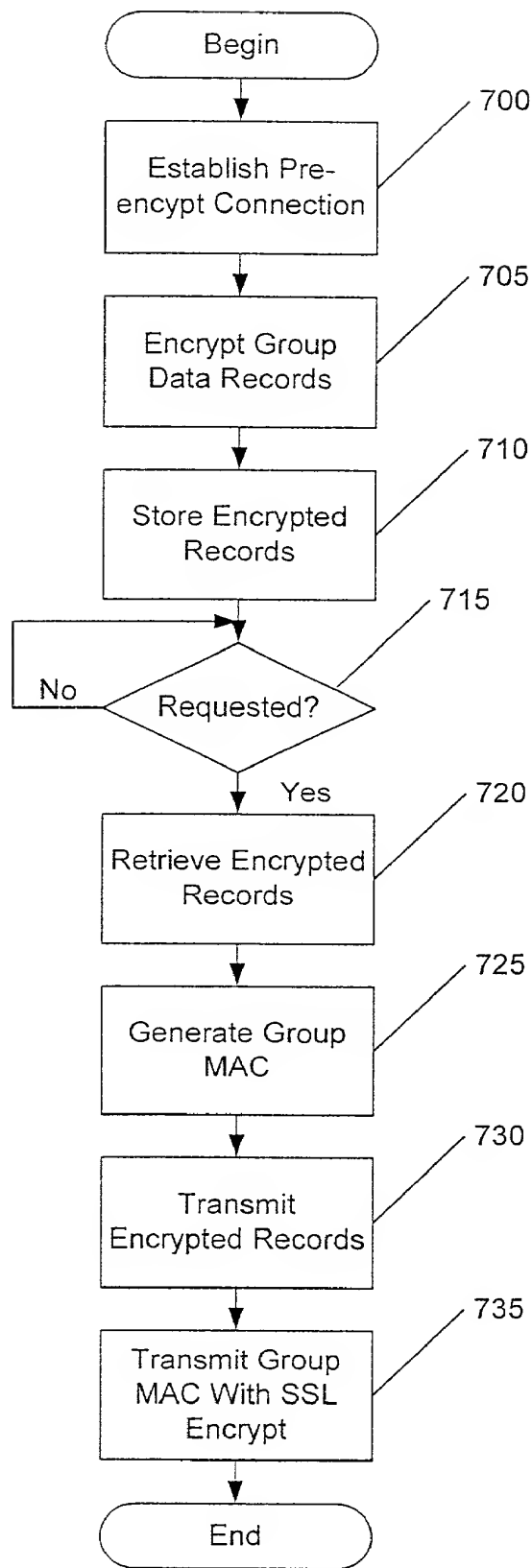


Figure 7

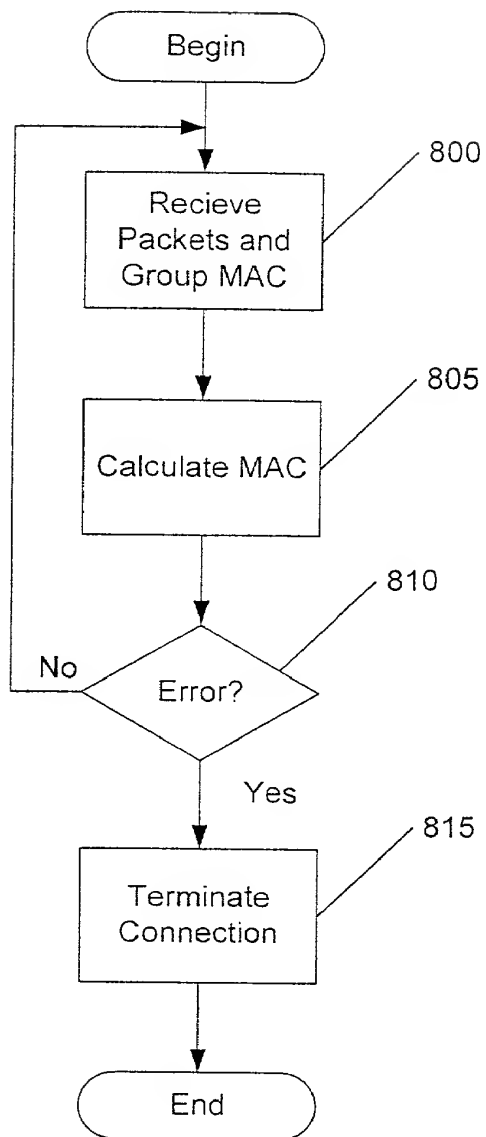


Figure 8

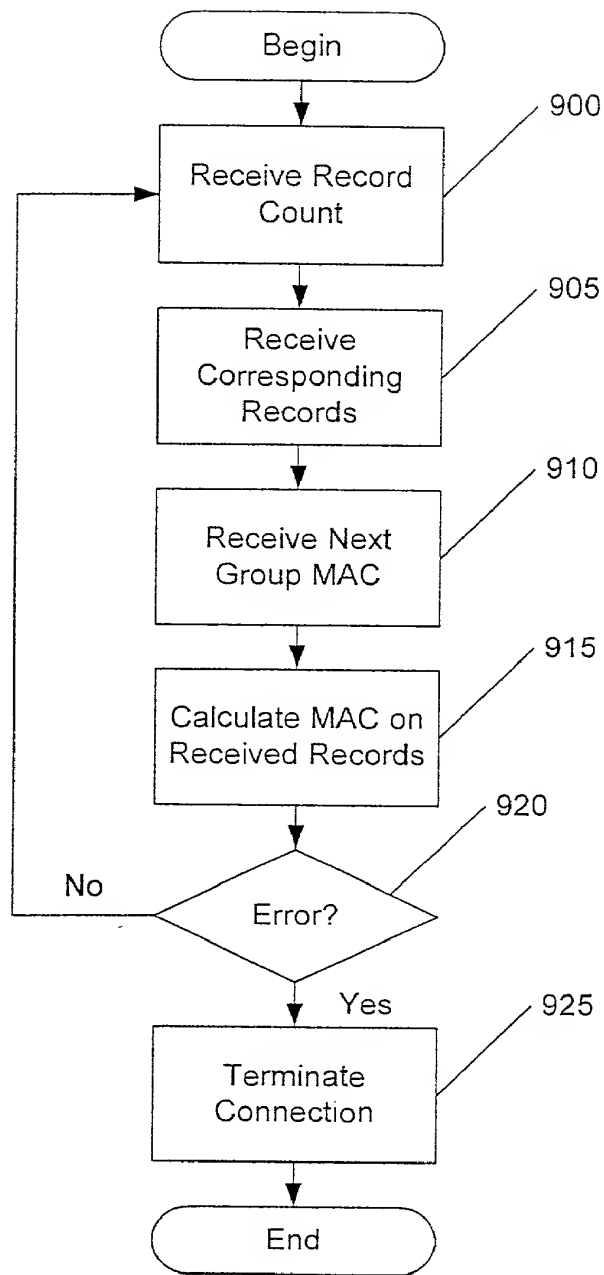


Figure 9

1 C → S: Client Hello With Delayed MAC Ciphersuite
2 S → C: Server Hello Selecting Delayed MAC Ciphersuite
3 C → S: (len to MAC=10) nnnnnnnnnnnMAC
4 S → C: (len to MAC=20) nnnnnnnnnnn
5 S → C: nnnnnnnnnnnMAC (len to MAC=15) nnnnn
6 S → C: nnnnnnnnnnnMAC
7 C → S: (len to MAC=10) nnnnnnnnnnnMAC
8 S → C: (len to MAC=30) nnnnnnnnnnn
9 S → C: nnnnnnnnnnn
10 S → C: nnnnnnnnnnnMAC
Close Session

Figure 10A

1 C → S: Client Hello With Delayed MAC No Encrypt Ciphersuite
2 S → C: Server Hello Selecting Delayed MAC No Encrypt Ciphersuite
3 C → S: (len to MAC=10) eeeeeeeeeeMAC
4 S → C: (len to MAC=20) eeeeeeeeee
5 S → C: eeeeeeeeeeMAC (len to MAC=15) eeeee
6 S → C: eeeeeeeeeeMAC
Close Session

Figure 10B

1 C → S: Client Hello With Delayed MAC and pre-encrypt key
2 S → C: Server Hello Selecting Delayed MAC and pre-encrypt key
3 C → S: (key) (len to MAC=10) eeeeeeeMAC
4 S → C: (key) (len to MAC=20) eeeeeee
5 S → C: eeeeeeeMAC (key) (len to MAC=15) eeeee
6 S → C: eeeeeeeMAC
Close Session

Figure 10C